**REPORT**

**Attacks on web application with and without the AWS WAF**

**Attack Vector 1: Large attachment size**

**Reason:**

There is a possibility that when a user uploads an attachment, they are not aware of the file size that is allowed.Also, sometime they accidently attach a file format that is not supported. This results in impacting the performance and eventually impacting credibility and efficiency of the application. So, we should stop the users from uploading such files using firewall. This will keep the application up and running efficiently. We have demonstrated this by considering the request body size restrictions.

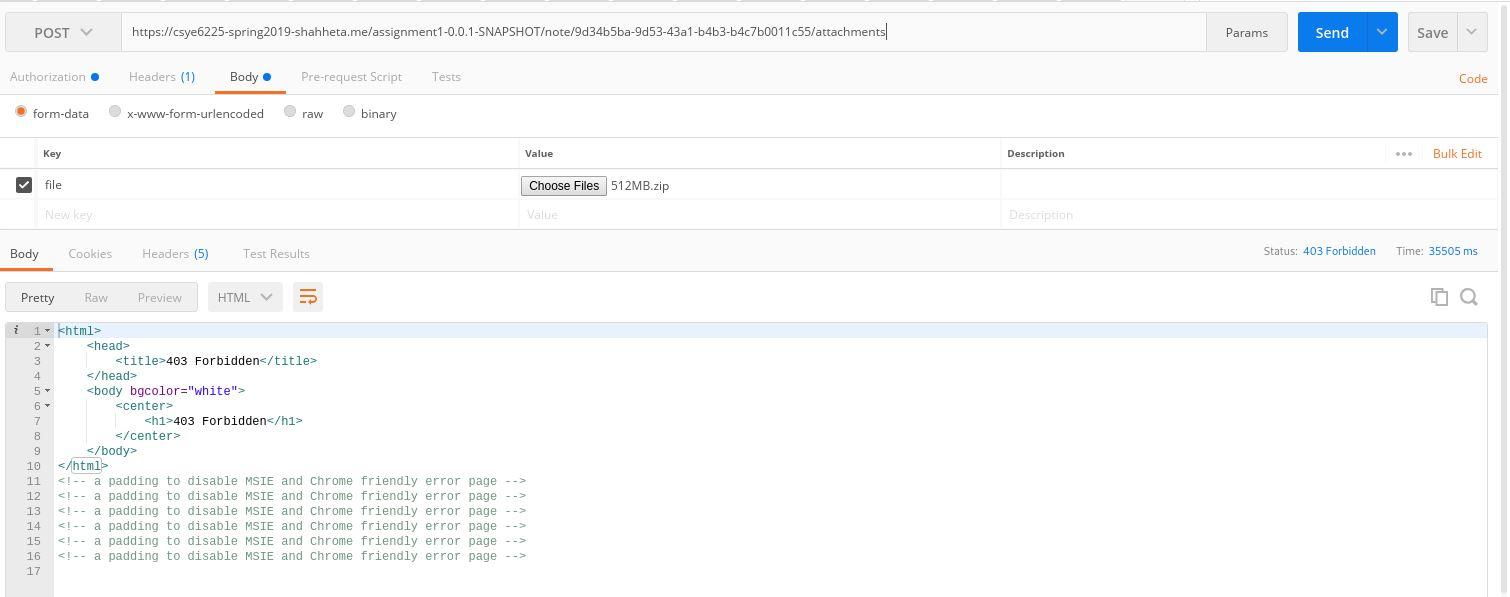
**Testing:**

Here we are trying to upload a file of 500MB for out attachment to the note. It will give us the file size error. In this test, we pass large sized files in a well written code, these files should not be attached to the note because they might induce considerable latency on our instances.



**Result:**

After setting up the Web Application Firewall, the firewall checks on the request body size and restricts user from uploading big files before letting the request reach the application.



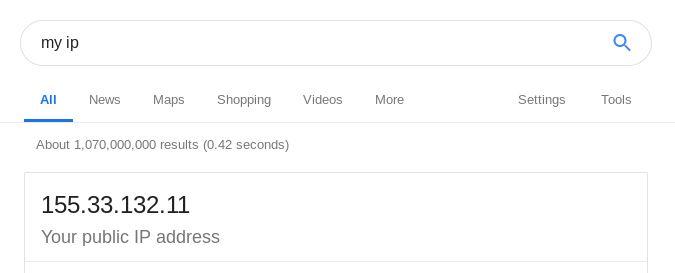
**Attack Vector 2: Blacklisted the unauthorized IP Address**

**Reason:**

The applications nowadays are very prone to getting hacked or be a victim of malicious data and unwanted requests so as to leak the confidential information. The IP addresses from where such attempts are being made should be monitored and blocked.

**Testing :**

We will run the application with your IP and domain name of the application. If the application returns a message in the form of json, your IP address is not in the blocked IP address list. But, if the application returns a “403 Forbidden” message, your IP has been blocked by the server.





**Result:**

Using AWS WAF, we were able to block the unwanted users by setting IP addresses or ranges of IP addresses to the block list. The requests and fake transactions from such IPs are blocked.

Here, IP address is 155.33.132.11 which is put under blocked IP list.

